INFORMATION SECURITY POLICY

ISO 27002	5.1
Author:	Chris Stone
Owner:	Ruskwig
Organisation:	TruePersona Ltd
Document No:	SP- 5.1
Version No:	1.0
Date:	10th January 2010

Document Control

Document Storage

Document Title Information Security Policy
Document Location C:\www\Ruskwig\docs\iso-27002\Information Security Policy.doc

Version History

Version No	Version Date	Author	Summary of Changes
1.0	10/01/2010	Chris Stone	First Issue

Approvals

Name	Title	Date of Approval	Version No
Chris Stone	Director	10/01/2010	1.0

Distribution

Name	Title	Date of Issue	Version No
Everyone	Internet	10/01/2010	1.0

Contents

0. Introduction

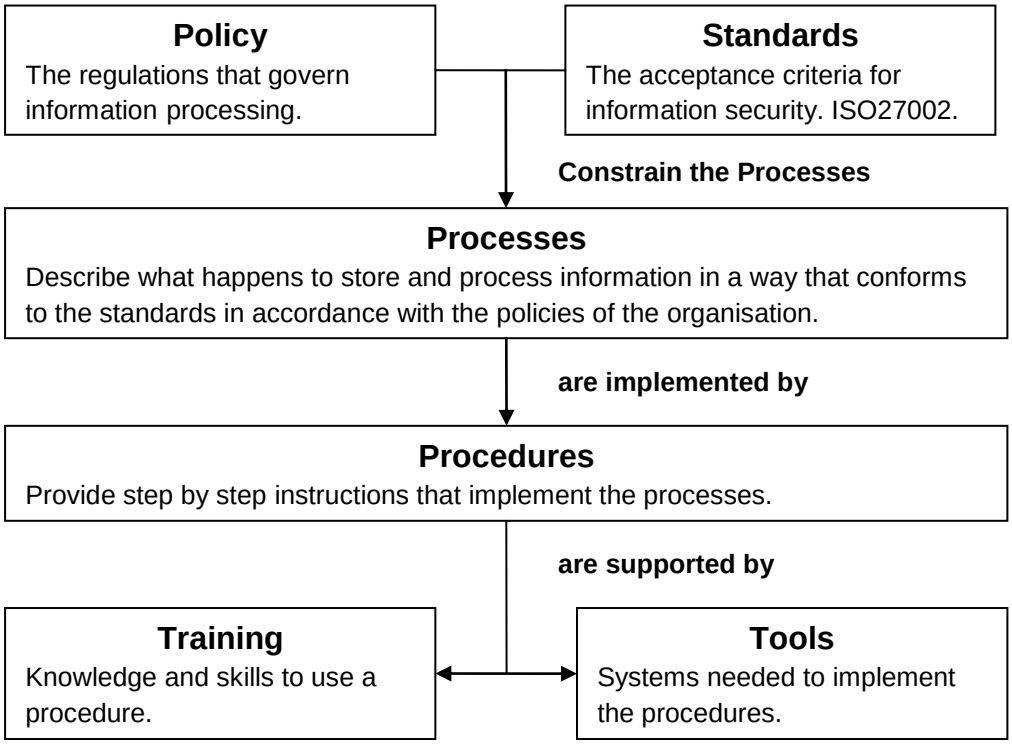
1.1 Information is an asset that the organisation has a duty and responsibility to protect. The availability of complete and accurate information is essential to the organisation functioning in an efficient manner and to providing products and services to customers.

1.2 The organisation holds and processes confidential and personal information on private individuals, employees, partners and suppliers and information relating to its own operations. In processing information the organisation has a responsibility to safeguard information and prevent its misuse.

1.2 The purpose and objective of this Information Security Policy is to set out a framework for the protection of the organisation's information assets:

- to protect the organisation's information from all threats, whether internal or external, deliberate or accidental,
- to enable secure information sharing,
- to encourage consistent and professional use of information,
- to ensure that everyone is clear about their roles in using and protecting information,
- to ensure business continuity and minimise business damage,
- to protect the organisation from legal liability and the inappropriate use of information.

1.3 The Information Security Policy is a high level document, and adopts a number of controls to protect information. The controls are delivered by policies, standards, processes, procedures, supported by training and tools.



1. Scope

2.1 This Information Security Policy outlines the framework for management of Information Security within the organisation.

2.2 The Information Security Policy, standards, processes and procedures apply to all staff and employees of the organisation, contractual third parties and agents of the organisation who have access to the organisation's information systems or information.

2.3 The Information Security Policy applies to all forms of information including:

- speech, spoken face to face, or communicated by phone or radio,
- hard copy data printed or written on paper,
- information stored in manual filing systems,
- communications sent by post / courier, fax, electronic mail,
- stored and processed via servers, PC's, laptops, mobile phones, PDA's,
- stored on any type of removable media, CD's, DVD's, tape, USB memory sticks, digital cameras.

2. Terms and Definitions

2.1 For the purpose of this document the following terms and definitions apply.

2.2 Asset
Anything that has value to the organization

2.3 Control
Means of managing risk, including policies, procedures, guidelines, practices

2.4 Guideline
A description that clarifies what should be done and how

2.5 Information Security
Preservation of confidentiality, integrity and availability of information

2.6 Policy
Overall intention and direction as formally expressed by management

2.7 Risk
Combination of the probability of an event and its consequence

2.8 Third Party
Person or body that is recognised as being independent

2.9 Threat
Potential cause of an unwanted incident, which may result in harm to a system

2.10 Vulnerability
Weakness of an asset that can be exploited by one or more threats

3. Structure of this Policy

3.1 This policy is based upon ISO 27002 and is structured to include the 11 main security category areas within the standard.

3.2 This policy is a high level policy which is supplemented by additional security policy documents which provide detailed policies and guidelines relating to specific security controls.

4. Risks

4.1 Data and information which is collected, analysed, stored, communicated and reported upon may be subject to theft, misuse, loss and corruption.

4.2 Data and information may be put at risk by poor education and training, misuse, and the breach of security controls.

4.3 Information security incidents can give rise to embarrassment, financial loss, non-compliance with standards and legislation as well as possible judgements being made against the organisation.

4.4 The organisation will undertake risk assessments to identify, quantify, and prioritise risks. Controls will be selected and implemented to mitigate the risks identified.

4.5 Risk assessments will be undertaken using a systematic approach to identify and estimate the magnitude of the risks.

5. Security Policy

5.1 Information Security Policy Document

5.1.1 The information security policy document sets out the organisations approach to managing information security.

5.1.2 The information security policy is approved by management and is communicated to all staff and employees of the organisation, contractual third parties and agents of the organisation.

5.2 Review

5.2.1 The security requirements for the organisation will be reviewed at least annually by the Head of IT and approved by the Board. Formal requests for changes will be raised for incorporation into the Information Security Policy, processes, and procedures.

6. Organisation of Information Security

6.1 Statement of Management intent

6.1.1 It is the policy of the organisation to ensure that Information will be protected from a loss of:

- Confidentiality: so that information is accessible only to authorised individuals.
- Integrity: safeguarding the accuracy and completeness of information and processing methods.
- Availability: that authorised users have access to relevant information when required.

6.1.2 The Head of IT will review and make recommendations on the security policy, policy standards, directives, procedures, Incident management and security awareness education.

6.1.3 Regulatory, legislative and contractual requirements will be incorporated into the Information Security Policy, processes and procedures.

6.1.4 The requirements of the Information Security Policy, processes, and procedures will be incorporated into the organisation's operational procedures and contractual arrangements.

6.1.5 The organisation will work towards implementing the ISO27000 standards, the International Standards for Information Security.

6.1.6 Guidance will be provided on what constitutes an Information Security Incident.

6.1.7 All breaches of information security, actual or suspected, must be reported and will be investigated.

6.1.8 Business continuity plans will be produced, maintained and tested.

6.1.9 Information security education and training will be made available to all staff and employees.

6.1.10 Information stored by the organisation will be appropriate to the business requirements.

6.2 Information Security Coordination

6.2.1 The security of information will be managed within an approved framework through assigning roles and co-ordinating implementation of this security policy across the organisation and in its dealings with third parties.

6.2.2 Specialist external advice will be drawn upon where necessary so as to maintain the Information Security Policy, processes and procedures to address new and emerging threats and standards.

6.3. Information Security Responsibilities

6.3.1 The Head of IT is the designated owner of the Information Security Policy and is responsible for the maintenance and review of the Information Security Policy, processes and procedures.

6.3.2 Heads of Department are responsible for ensuring that all staff and employees, contractual third parties and agents of the organisation are made aware of and comply with the Information Security Policy, processes and procedures.

6.3.3 The organisation's auditors will review the adequacy of the controls that are implemented to protect the organisation's information and recommend improvements where deficiencies are found.

6.3.4 All staff and employees of the organisation, contractual third parties and agents of the organisation accessing the organisation's information are required to adhere to the Information Security Policy, processes and procedures.

6.3.5 Failure to comply with the Information Security Policy, processes and procedures will lead to disciplinary or remedial action.

7. Asset Management

7.1 The organisation's assets will be appropriately protected.

7.2 All assets (data, information, software, computer and communications equipment, service utilities and people) will be accounted for and have an owner.

7.2 Owners will be identified for all assets and they will be responsible for the maintenance and protection of their assets.

8. Human Resources Security

8.1 The organisations security policies will be communicated to all employees, contractors and third parties to ensure that they understand their responsibilities.

8.2 Security responsibilities will be included in job descriptions and in terms and conditions of employment.

8.3 Verification checks will be carried out on all new employees, contractors and third parties.

9. Physical and Environmental Security

9.1 Critical or sensitive information processing facilities will be housed in secure areas.

9.2 The secure areas will be protected by defined security perimeters with appropriate security barriers and entry controls.

9.3 Critical and sensitive information will be physically protected from unauthorised access, damage and interference.

10. Communications and Operations Management

10.1 The organisation will operate its information processing facilities securely.

10.1 Responsibilities and procedures for the management, operation and ongoing security and availability of all data and information processing facilities will be established.

10.2 Appropriate operating procedures will be put in place.

10.3 Segregation of duties will be implemented, where appropriate, to reduce the risk of negligent or deliberate system misuse

11. Access Control

11.1 Access to all information will be controlled.

11.1 Access to information and information systems will be driven by business requirements. Access will be granted or arrangements made for employees, partners, suppliers according to their role, only to a level that will allow them to carry out their duties.

11.2 A formal user registration and de-registration procedure will be implemented for access to all information systems and services.

12. Information Systems Acquisition, Development, Maintenance

12.1 The information security requirements will be defined during the development of business requirements for new information systems or changes to existing information systems.

12.2 Controls to mitigate any risks identified will be implemented where appropriate.

13. Information Security Incident Management

13.1 information security incidents and vulnerabilities associated with information systems will be communicated in a timely manner. Appropriate corrective action will be taken.

13.2 Formal incident reporting and escalation will be implemented.

13.3 All employees, contractors and third party users will be made aware of the procedures for reporting the different types of security incident, or vulnerability that might have an impact on the security of the organisation's assets.

13.4 Information security incidents and vulnerabilities will be reported as quickly as possible to the ICT Service desk.

14. Business Continuity Management

14.1 The organisation will put in place arrangements to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

14.2 A business continuity management process will be implemented to minimise the impact on the organisation and recover from loss of information assets. Critical business processes will be identified.

14.3 Business impact analysis will be undertaken of the consequences of disasters, security failures, loss of service, and lack of service availability.

15. Compliance

15.1 The organisation will abide by any law, statutory, regulatory or contractual obligations affecting its information systems.

15.1 The design, operation, use and management of information systems will comply with all statutory, regulatory and contractual security requirements.